REMARKS

Claims 1-5, 9-22, 24-29 and 32 are currently pending in the subject application and are presently under consideration. Claims 1, 4, 10, 11, 17, 18, 20-22, 24-26, and 28 have been amended as shown on pages 5-11 of the Reply. In addition, the specification has been amended as indicated on pages 2-4.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-5, 9-16, and 32 Under 35 U.S.C. §102(e)

Claims 1-5, 9-16, and 32 are rejected under 35 U.S.C. §102(e) as being anticipated by Salowey (U.S. Patent 7,370,350). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Salowey does not disclose or suggest each and every feature of the subject claims.

> For a prior art reference to anticipate, 35 U.S.C. §102 requires that "each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950 (Fed. Cir. 1999) (*quoting Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)).

The subject application relates to extension of factory communication protocols to include automation security and intrusion detection capabilities. This can include adapting factory protocols such as Control and Information Protocol (CIP), Fieldbus, Modbus, and the like to include encoded security components that provide varying levels of automation security within a control network. One such adaptation can comprise extending a path definition within a factory protocol to include a segment or security field identifying a requester of a connection between automation devices. The security field can be employed by the automation system to authenticate the requestor prior to allowing communication between the devices. In particular, amended independent claim 1 recites, *an extensible factory protocol to transport data between the automation asset and a remote automation asset on a remote network communication channel, the extensible factory protocol is* ***a control-specific transport mechanism for data exchange between automation assets that is adapted to include at least one security field***

within the extensible factory protocol *to exchange data with the remote automation asset,* ***the security field of the extensible factory protocol authenticates at least one of a requestor of the data or a supplier of the data.***

Salowey does not contemplate adapting a control-specific factory protocol to include such security components. Salowey relates to a technique for re-authenticating networked devices to one another using short-term authentication. According to this technique, a client is issued a temporary authentication key upon initial authentication with a server. If later re-authentication of the client is necessary (as a result of a client reboot, relocation of the client, or other such event), the re-authentication can be effected using a challenge-response exchange between the client and the server based on the temporary authentication key. Asserting that Salowey discloses the extensible factory protocol of independent claim 1, the Office Action notes in particular that initial authentication of a client according to Salowey is performed using Extensible Authentication Protocol (EAP), wherein an authentication center maintains data used to authenticate particular mobile devices, and messages are exchanged between this authentication center and a mobile device desiring communication with a server or other device.

However, the cited EAP authentication exchange is performed between a first computing device (*e.g.* the mobile device) and the *above-mentioned authentication center* in order to authenticate communication between the first computing device and a second computing device. By contrast, the extensible factory protocol of amended independent claim 1 comprises a control-specific transport mechanism for data exchange *between automation assets*, the control-specific transport mechanism being *adapted to include at least one security field within the extensible factory protocol*. Salowey is silent regarding a *factory protocol* that has been *adapted to include at least one security field*, since the cited reference does not contemplate factory protocols in any context. More specifically, Salowey does not disclose that such a factory protocol adaptation can include a *security field that authenticates at least one of a requestor of the data or a supplier of the data*. By providing such extensible factory protocols, the present invention can cleanly integrate security mechanisms within a control-specific factory network environment. Salowey's re-authentication system does not provide these benefits.

Providing a particular factory protocol extension according to one or more embodiments of the present application, amended claim 10 recites, *the extensible factory protocol comprises a Control and Information Protocol (CIP) having a path segment that has been adapted to include* *a segment identifying a requestor of a connection between automation assets and employed to authenticate the requestor*. As already discussed, Salowey does not disclose or suggest adapting a factory protocol to include at least one security field. The cited reference therefore fails to disclose in particular *a CIP protocol having a path segment that has been adapted to include a segment identifying a requestor of a connection*.

In view of at least the foregoing, it is respectfully submitted that Salowey does not disclose each and every feature set forth in amended independent claim 1 (and all claims depending there from), and as such fails to anticipate or render obvious the present invention. It is therefore requested that this rejection be withdrawn.

II. Rejection of Claims 17-24 Under 35 U.S.C. §103(a)

Claims 17-24 are rejected under 35 U.S.C. §103(a) as being unpatentable over Salowey, in view of Branstad, *et al.* (U.S. Patent 6,842,860). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Salowey and Branstad, *et al.*, individually or in combination, do not disclose all aspects of the subject claims.

> To reject claims in an application under § 103, an examiner must establish a prima facie case of obviousness. A prima facie case of obviousness is established by a showing of three basic criteria. First, there must be some apparent reason to combine the known elements in the fashion claimed by the patent at issue (*e.g.*, in the references themselves, interrelated teachings of multiple patents, the effects of demands known to the design community or present in the marketplace, or in the knowledge generally available to one of ordinary skill in the art). To facilitate review, this analysis should be made explicit. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. See MPEP § 706.02(j). See also KSR Int'l Co. v. Teleflex, Inc., 550 U.S. 398, 04-1350, slip op. at 14 (2007). The reasonable expectation of success must be found in the prior art and not based on applicant's disclosure. See In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)

In addition to the features already discussed, one or more embodiments of the present application can vary the level of security used to protect communications between automation devices in accordance with the real-time data transfer requirements of the devices. That is, a lightweight, less computationally intensive security mechanism can be employed when real-time data performance is a priority, while a more intensive security mechanism can be applied when real-time data transfer performance is less critical. To this end, performance requirements for the automation devices can be evaluated, and an appropriate level of security for communication between the devices can be negotiated. In addition, the security protocol used to protect these communications can include an encoded component that times-out communications between the devices after a predetermined amount of time and causes a subsequent renegotiation of security levels before subsequent data transactions between the devices are allowed. In this way, the level of security for automation device transactions can vary dynamically according to the current real-time data performance requirements. In particular, amended independent claim 17 recites, *providing a security time-out within the wireless security protocol that times-out data transactions between the automation devices after a predetermined time duration until a subsequent determination of real-time data transfer requirements and network security requirements is performed.*

Salowey does not contemplate varying levels of security based on a real-time data performance requirement, and therefore does not disclose encoding a security time-out within a security protocol that enforces re-determination of such security levels. Branstad, *et al.* is also silent regarding these aspects. Branstad, *et al.* relates to a network authentication system that dynamically selects an authentication mechanism having a strength level in accordance with current security conditions and processor loading. The strength of authentication mechanism selected for use can be dynamically adjusted as observed security or computing conditions change. However, Branstad, *et al.* does not employ *a security time-out that times-out data transactions between devices after a predetermined time duration* until a subsequent determination of real-time data transfer requirements and network security requirements is performed. Rather, Branstad, *et al.* employs periodic heartbeat messages sent from a receiver device to a sender device that contain information regarding authentication errors, CPU load information, missing packet information, and the like. The sender employs this heartbeat information to determine whether the authentication strength level should be adjusted in response to changing conditions. This heartbeat technique for adjusting an authentication level is clearly distinct from, and in no way suggests, the *security time-out* of amended independent claim 17.

Similarly, amended independent claim 20 recites, *providing a security time-out within the security protocol that times-out the communications session after a predetermined amount of* *time until a subsequent determination for real-time communication is made*, and as discussed *supra*, neither Salowey nor Branstad, *et al.* discloses or suggests such a security time-out.

Likewise, amended independent claim 24 recites, *means for enforcing a time limit on data exchange between the automation asset in the control domain and the automation asset remote to the domain, after which time limit the data exchange is timed-out until the performance parameter is re-determined.* Salowey and Branstad, *et al.* are silent regarding these aspects, as already discussed.

In view of at least the foregoing, it is respectfully submitted that Salowey and Branstad, *et al.*, individually or in combination, do not disclose all aspects of amended independent claims 17, 20, and 24 (and all claims depending there from), and as such fail to make obvious the subject invention. It is therefore requested that this rejection be withdrawn.

III. **Rejection of Claims 25-29 Under 35 U.S.C. §103(a)**

Claims 25-29 are rejected under 35 U.S.C. §103(a) as being unpatentable over Salowey, in view of Branstad, *et al.*, and further in view of Bridges, *et al.* ("Al Techniques Applied to High Performance Computing Intrusion Detection"). However, amended independent claim 25 recites, *a time component encoded in the factory protocol that defines an amount of time after which data exchange between control devices is timed-out until the at least one of a security or performance parameter is re-evaluated*, and as discussed in the previous section of the Reply, Salowey and Branstad, *et al.* fail to disclose or suggest such a time component. Bridges, *et al.* fails to remedy these deficiencies. Bridges, *et al.* relates to the use of artificial intelligence techniques in intrusion detection mechanisms, but does not disclose or suggest encoding a time component within a factory protocol that *defines an amount of time after which data exchange between control devices is timed-out until a security or performance parameter is re-evaluated.*

Also, independent claim 28, as amended, recites, *providing a time-based component within the industrial network protocol that defines an amount of time after which the real-time performance must be re-evaluated before data transactions between the automation devices are allowed to continue.* None of the cited references disclose such a time-based component, as noted *supra*.

In view of at least the foregoing, it is respectfully submitted that Salowey, Branstad, *et al.*, and Bridges, *et al.*, individually or in combination, do not disclose or suggest all features set forth in amended independent claims 25 and 28 (and all claims depending there from), and as such fail to make obvious the present invention. It is therefore requested that this rejection be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [ALBRP303USB].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,
TUROCY & WATSON, LLP

/Brian Steed/
Brian Steed
Reg. No. 64,095

TUROCY & WATSON, LLP
127 Public Square
57th Floor, Key Tower
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731